

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	P. HODGES ET AL.: "A FAST MODULAR DIVISION METHOD" IBM TECHNICAL DISCLOSURE BULLETIN., vol. 12, no. 7, December 1969 (1969-12), pages 1040-1041, XP002301376 USIBM CORP. NEW YORK. the whole document	1-33
X	GOLOMB S W ET AL: "INTEGER CONVOLUTIONS OVER THE FINITE FIELD GF(3.2N+1)" SIAM JOURNAL OF APPLIED MATHEMATICS, vol. 32, no. 2, March 1977 (1977-03), pages 356-365, XP001197219 page 360	1-33
X	US 5 463 690 A (CRANDALL RICHARD E) 31 October 1995 (1995-10-31) abstract; figures 5,7	1-33

-/--

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Z* document member of the same patent family

Date of the actual completion of the international search

19 October 2004

Date of mailing of the international search report

02/11/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Verhoof, P

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PIESTRAK S J: "DESIGN OF RESIDUE GENERATORS AND MULTIOPERAND MODULAR ADDERS USING CARRY-SAVE ADDERS" IEEE TRANSACTIONS ON COMPUTERS, vol. 43, no. 1, 1994, pages 68-77, XP000418592 IEEE NEW YORK, NY, USA ISSN: 0018-9340 sections IV.A, IV.C -----	1-33
A	TOMAHECHI N ET AL: "Pipelined design of the high-speed RSA encryption processor with built-in table for residue calculation of redundant binary numbers" IEEE TENCON' 02. 2002 IEEE REGION 10 CONFERENCE ON COMPUTERS, COMMUNICATIONS, CONTROL AND POWER ENGINEERING PROCEEDINGS. BEIJING, CHINA, OCT. 28 - 31, 2002, IEEE REGION 10 ANNUAL CONFERENCE, NEW YORK, NY : IEEE, US, vol. VOL. 1 OF 3, 28 October 2002 (2002-10-28), pages 412-415, XP010628511 ISBN: 0-7803-7490-8 figure 1 -----	10,27
A	US 5 126 963 A (FUKASAWA HISAKO) 30 June 1992 (1992-06-30) column 6, line 1 - column 7, line 8; figure 3 -----	10,27

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5463690	A	31-10-1995	US 5271061 A	14-12-1993
			US 5159632 A	27-10-1992
			US 6049610 A	11-04-2000
			US 5581616 A	03-12-1996
			US 6285760 B1	04-09-2001
			US 5805703 A	08-09-1998
			US 6307935 B1	23-10-2001
			US 2002122555 A1	05-09-2002
			AU 2697792 A	27-04-1993
			WO 9306672 A1	01-04-1993
US 5126963	A	30-06-1992	JP 2055530 C	23-05-1996
			JP 2306337 A	19-12-1990
			JP 7092739 B	09-10-1995